Exhibit A

NO. *Court File No.* ***VLC-S-S-246520***

VANCOUVER REGISTRY

IN THE SUPREME COURT OF BRITISH COLUMBIA

BETWEEN:

J. R. and M. M.

PLAINTIFFS

AND:

23ANDME HOLDING CO., and 23ANDME, INC.,
ANNE WOJCICKI, ROELOF BOTHA, PATRICK CHUNG,
PETER J. TAYLOR, DAVID BAKER and KPMG LLP (UNITED STATES)

DEFENDANTS

NOTICE OF CIVIL CLAIM

Brought under the *Class Proceedings Act*, RSBC 1996, c. 50

This action has been started by the Plaintiffs for the relief set out in Part 3 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the Plaintiff,

(a) if you were served with the notice of civil claim anywhere in Canada, within 21 days after that service,

(b) if you were served with the notice of civil claim anywhere in the United States of America, within 35 days after that service,

(c) if you were served with the notice of civil claim anywhere else, within 49 days after that service, or

(d) if the time for response to civil claim has been set by order of the court, within that time.

[the balance of this page has been intentionally left blank]

CLAIM OF THE PLAINTIFFS

PART 1: STATEMENT OF FACTS

A. NATURE OF THE ACTION

1. This proposed privacy class action arises out of a data breach that affected the 23andMe Defendants' customers in 2023 (hereinafter, "**Data Breach**").

2. The Data Breach occurred over the span of approximately five months—between April 29 and September 27, 2023. The Data Breach, which was reported in October 2023, resulted in the theft or compromise of highly sensitive and highly valuable personal information of millions of customers of the 23andMe Defendants, including information regarding their ethnicities, religious backgrounds, ancestry roots and connections, and genetics.

3. 23andMe Defendants' customer data was posted for sale on the Dark Web in several tranches between August and October 2023. In October 2023, cybercriminals made available the information of approximately 5.1 million of the 23andMe Defendants' customers for sale on the Dark Web. This followed an initial posting on the Dark Web made in August 2023, where cybercriminals claimed to possess 300 terabytes of stolen data on the 23andMe Defendants' customers.

4. The Defendants describe themselves as the pioneers in direct-to-consumer genetic testing, and have accumulated a vast database of human genome, amongst other highly sensitive and valuable personal and personally identifiable information.

5. The Defendants acknowledge that they are subject to rigorous data privacy and data protection regulation in the jurisdictions in which they operate, including in Canada.

6. At all times, the Defendants have been cognizant of the fact that they collect and/or generate highly sensitive personal information with respect to their customers, the theft or compromise of which would have far reaching consequences for customers.

7. At all times, the Defendants consistently promised, stated and represented that "At 23andMe, Privacy is in our DNA." They represented that they utilized appropriate and adequate data retention and data protection measures to protect customers' privacy, and to safeguard their highly sensitive and highly valuable personal information against unauthorized access or theft.

8. This action arises out of two main allegations:

   a. **IMPROPER DATA RETENTION MEASURES AND PRACTICES:** first, that contrary to their promises, statements and representations, as well as the standards applicable to them by virtue of privacy regulation and practices, the 23andMe Defendants did not introduce, implement and/or maintain proper data retention practices. As a result, they retained a significant volume of highly sensitive customer information outside of the scope of their authorization; and

   b. **IMPROPER DATA PROTECTION MEASURES AND PRACTICES:** second, that contrary to their promises, statements and representations, as well as the standards applicable to them by virtue of privacy regulation and industry practices, the 23andMe Defendants did not introduce, implement and/or maintain proper data protection measures and/or practices. As a result, they affirmatively exposed the highly sensitive and highly valuable customer data in their control, custody or possession to unauthorized parties and cybercriminals.

9. This action alleges that the 23andMe Defendants failed to conduct their data retention and protection practices appropriate to the sensitivity of the customer

information in their power, custody or possession, or the severity of the risk of cyberattacks. The Defendants' conduct was willful, knowing or reckless.

10. This action alleges that the 23andMe Defendants' actions and omissions in breach of their duties were deliberate and purposeful, and were carried out in the normal course of the 23andMe Defendants' commercial activities and in furtherance of their business interests. The Individual Defendants and KPMG acted together with the 23ande Defendants as co-principals and/or co-conspirators, and materially contributed to the Data Breach and the violation of customers' privacy. But for the actions, omissions and breaches of duties on the parts of each of the Defendants, the Data Breach would not have occurred. The Data Breach was the product of the Defendants' knowing or, alternatively, reckless, thus willful conduct.

11. The Plaintiff has brought this proposed multijurisdictional class proceeding on behalf of himself and a putative Class defined as follows:

> All natural persons residing or domiciled in Canada whose sensitive personal information was accessed by unauthorized parties or otherwise compromised in the course of or as a result of the Data Breach;
>
> Excluded from the Class are the directors, partners, officers or senior employees of the Defendants or any of their subsidiaries;
>
> (hereinafter, the "**Class**" or "**Class Members**").

12. The Plaintiff and the putative Class Members have incurred and will continue to incur harms, damages, and losses as a result of the Defendants' conduct, including for the price they paid for the Defendants' offerings and services, and the further harms, damages and losses resulting from the Data Breach and its far-reaching consequences.

13. The Plaintiffs asserts and advances the following causes of action:

a. Breaches of Provincial Privacy Legislation (against all Defendants);

b. Intrusion upon seclusion (against all Defendants);

c. Breaches of Provincial Consumer Legislation (against 23andMe Holding Co and 23andMe, Inc.);

d. Breach of contract (against 23andMe Holding Co and 23andMe, Inc.);

e. Negligence (against all Defendants); and

f. Breach of the *Competition Act* (against all Defendants);

as such terms are defined and the claims particularized herein at Part 2.

14. This proposed class proceeding seeks to recover compensation for the benefit of the Plaintiffs and the putative Class Members under statutory, common law and/or equitable headings of damages.

PART 2: STATEMENT OF FACTS

B. The Plaintiffs

15. The Plaintiff, J. R., is a resident of British Columbia. On or about October 9, 2023, he received a notification email from the Defendants in relation to the Data Breach. J. R. has Eastern European Jewish connections, and was extremely concerned to receive the news that 23andMe's customers' data had been breached and posted on the Dark Web. To date, J. R. has not received meaningful communication from the 23andMe Defendants regarding the impact of the Data Breach on him.

16. The Plaintiff, M. M., is a resident of Ontario. M. M. is an individual with the Ashkenazi Jew heritage. On or about October 8, 2023, she learned through the media that hackers had curated a list of 1 million Ashkenazi Jewish customers of 23andMe, and were selling that information on the Dark Web. Since then, M. M. has proactively attempted to obtain further information from the 23andMe

Defendants regarding the impact of the Data Breach on her, but those attempts have not been successful. To date, M. M. has not received meaningful communication from the 23andMe Defendants regarding the impact of the Data Breach on her. M. M. has suffered emotional harms as a result of the Data Breach.

C. The Proposed Class and Sub-Class

17. The Plaintiffs brings this proposed multijurisdictional class proceeding on their his own behalf and on behalf of a proposed Class and a proposed Sub-Class, which are defined as follows:

> All natural persons residing or domiciled in Canada whose sensitive personal information was accessed by unauthorized parties or otherwise compromised in the course of or as a result of the Data Breach;
>
> The Class includes the following **Sub-Class**: all natural persons residing or domiciled in Canada whose sensitive personal information was accessed by unauthorized parties or otherwise compromised in the course or as a result of the Data Breach, whose information was posted on the Dark Web;
>
> Excluded from the Class are the directors, partners, officers or senior employees of the 23andMe Defendants, KPMG or any of their respective subsidiaries;
>
> (hereinafter, the "**Class**" or "**Class Members**").

D. The Defendants

a) 23andaMe Defendants

18. The Defendant 23andMe Holding Co. is an entity continued under the laws of the State of Delaware, and based in South San Francisco, California.

19. 23andMe Holding Co. is a publicly traded company, and its stock is listed for trading on The NASDAQ Global Select Market under the ticker symbol “ME.”

20. The Defendant 23andMe, Inc. is a wholly-owned subsidiary of the Defendant 23andMe Holding Co. It is incorporated under the laws of Delaware, and based in South San Francisco, California.

21. In this Amended Notice of Civil Claim, the Defendants 23andMe Holding Co. and 23andMe, Inc. are collectively referred to as “**23andMe Defendants**.”

22. The 23andMe Defendants’ stated mission is “to help people access, understand, and benefit from the human genome.” According to the 23andMe Defendants, “[t]o achieve this, [they] are building the leading direct-to-consumer precision medicine platform that powers [their] genetics driven therapeutics and research business.”

23. The 23andMe Defendants describe themselves as the pioneers “in direct-to-consumer genetic testing, giving consumers unique, personalized information about their genetic health risks, ancestry, and traits.”

24. The 23andMe Defendants operate in two reporting business segments: Consumer & Research Services and Therapeutics.

25. In their Consumer and Research Services segment, the 23andMe Defendants offer two types of services:

    a. first, the Personal Genome Services (“**PGS**”): The 23andMe Defendants’ PGS services provide customers with a broad suite of genetic reports,

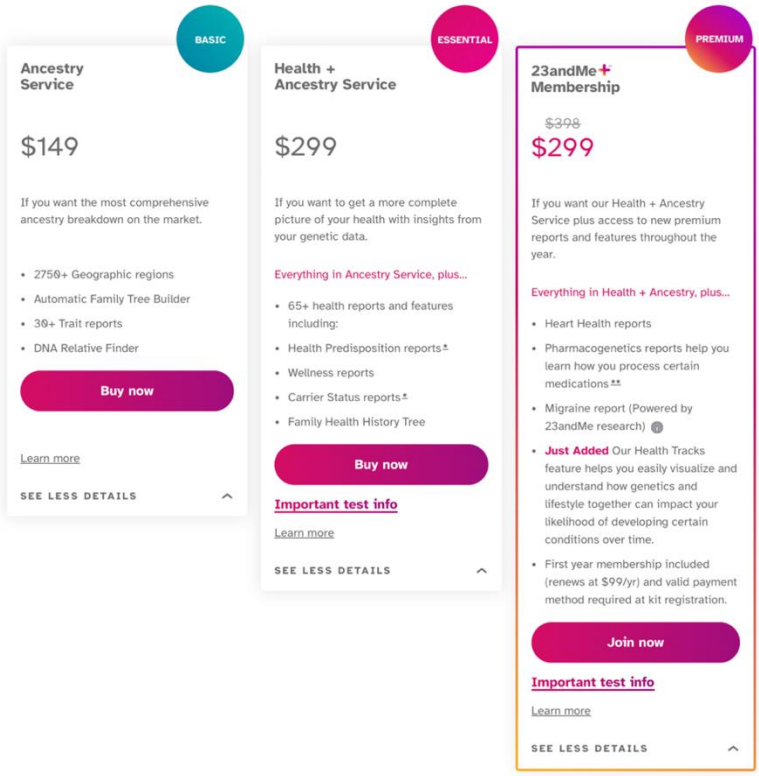
including information on customers' genetic ancestral origins, personal genetic health risks, and chances of passing on certain rare carrier conditions to their children, as well as reports on how genetics can impact responses to medications. These services are offered in various jurisdictions, including in Canada; and

b. second, Telehealth services: the 23andMe Defendants provide these services under their Lemonaid subsidiaries division and platform. These services purport to provide patients access to one of the 23andMe Defendants' affiliated licensed healthcare professionals for medical consultation and treatment for a number of common conditions, and telehealth consultations for certain 23andMe genetic reports.

26. In addition to its customer-facing services and offerings, the 23andMe Defendants engage in research services whereby they use their "vast database of genetic and phenotypic information provided by consenting customers to discover insights into the genetic origins of disease and to identify targets for drug development." According to the Defendants, over 80% of their customers elect to participate in the research program.

27. The 23andMe Defendants have monetized customer data for years through licensing them to pharmaceutical development companies. For example, in 2018, the 23andMe Defendants gave license to GlaxoSmithKline ("**GSK**"), a giant pharmaceuticals company, for US$300 million. Most recently, on November 3, 2023, days after the reports of the Data Breach, the 23andMe Defendants reported that they had extended a 5-year collaboration with GSK plc licensing 23andMe data for development of pharmaceuticals.

28. The 23andMe Defendants also generate revenue from their customers directly. They provide various tiers of services, and charge customers up to $398 for their offerings and services, plus additional annual membership fees, as seen in the snapshot provided below, which has been retrieved from the 23andMe Defendants' website.



29. According to the 23andMe Defendants, a substantially portion of their revenues is are derived from the PGS services, which represented approximately 68%, 75% and 81% of their total consolidated revenues for the fiscal years ended March 31, 2023, 2022 and 2021, respectively.

30. On information and belief, approximately 14 million individuals have shared their genetic information with the 23andMe Defendants. The 23andMe Defendants have since confirmed that, as of the occurrence of the Data Breach, they had approximately 14 million customers.

31. The 23andMe Defendants have been providing their offerings and services in Canada since October of 2014.

32. The below table, which has been retrieved from the 23andMe Defendants' filings with the United States Securities and Exchange Commission, provides a breakdown of the 23andMe Defendants' consolidated revenues in its various operating geographical markets:

	Year Ended March 31,					
	2023		2022		2021	
	Amount	% of Revenue	Amount	% of Revenue	Amount	% of Revenue
	(in thousands, except percentages)					
United States	$ 217,242	73%	$ 192,438	71%	$ 176,120	72%
United Kingdom	63,023	21%	58,477	22%	49,386	20%
Canada	13,581	4%	14,293	5%	12,172	5%
Other regions	5,643	2%	6,685	2%	6,242	3%
Total	$ 299,489	100%	$ 271,893	100%	$ 243,920	100%

33. On information and belief, the population of the 23andMe Defendants' Canadian customers is significant.

b) Individual Defendants

34. **Anne Wojcicki** is a Co-Founder of 23andMe, and she currently serves as the company's Chief Executive Officer, President, a Director and Chair of the Board of Directors of 23andMe Holding Co. Ms. Wojcicki co-founded 23andMe in 2006 together with two other individuals with the goal of providing common people access to their genetic information.

35. At all material times, Ms. Wojcicki has been aware of the privacy risks and concerns associated with building one of the largest databases of human genome. And she has made representations to the public regarding 23andMe Defendants' privacy practices. For instance, on or about September 21, 2021, the New York Times published an interview with Ms. Wojcicki, titled "What Is 23andMe Doing With Your DNA?" In this interview, Ms. Wojcicki boasted about 23andMe Defendants' practices, emphasizing that 23andMe's structure was built on an "opt-in" basis, and that it "always provide choice and transparency."

36. **Roelof Botha** is a director of 23andMe and a member of 23andMe's Board of Director's Audit Committee. According to 23andMe, Mr. Botha focuses on Internet, services and software investments, and he has significant experience being involved with several major tech companies.

37. **Patrick Chung** is a director of 23andMe and a member of 23andMe's Board of Director's Audit Committee. Mr. Chung is a highly experienced industry

professional, having been involved with several major consultancy and tech companies. Mr. Chung hold as joint JD-MBA degree from Harvard Law School and Harvard Business School, and is an attorney admitted to the practice of law in the States of New York and Massachusetts.

38. **Peter J. Taylor** is a director of 23andMe and a member of 23andMe's Board of Director's Audit Committee.

39. At the relevant time, **David Baker** was 23andMe's Chief Security Officer. Mr. Baker joined 23andMe in 2020 s Chief Security Officer and Vice President of Engineering, overseeing IT & Security for the company, and purportedly helping it set the industry standard for data privacy and security. Mr. Baker's name has been removed from the Leadership section of 23andMe's website. It is unclear whether or not he continues to hold a senior leadership, or any, position with 23andMe.

40. Mr. Baker has been closely involved with 23andMe's data privacy and cybersecurity efforts, and he has readily acknowledged both: (a) the sensitivity of the information in 23andMe's possession; and (b) the real and significant risk of harm arising from the compromise of that information. In an interview published in June 2021, titled "Data Privacy Is in 23andMe CSO's DNA," Mr. Baker acknowledged the significant value of the information in the possession of the 23andMe Defendants. He furthermore acknowledged the risk of significant harm arising from the compromise of that information, and that it can lead to "a comprehensive identify theft." During this interview, Mr. Baker furthermore made representations to the public regarding 23andMe's purportedly robust data privacy and security measures and practices,

41. The Individual Defendants are highly sophisticated business and industry leaders who have unparalleled experience with the tech industry.

42. As key directors and officers of 23andMe overseeing key and fundamental aspects of 23andMe's business, the Individual Defendants had a duty to

affirmatively take steps to ensure 23andMe complied with the applicable standards to safeguard the privacy of its customers' data.

43. Specifically, as part of their duties as officers and directors of 23andMe, the Individual Defendants had the overarching duty to assess the efficacy and propriety of the company's measures to ensure the privacy measures and practices of the company commensurate with the heightened cybersecurity and privacy risks.

44. The Individual Defendants' duty is outlined in the Charter of the Audit Committee of the Board of Directors of 23andMe, dated May 18, 2023, which states as follows:

> **D. Risk Management, Compliance and Ethics**
>
> **(i) Risk Management.** The Committee shall review and discuss with management, the head of the internal audit function, if any, and the independent auditor any significant financial, commercial, operational *(including cybersecurity, privacy, and information technology)*, regulatory, and strategic risks or exposures and the Company's policies and processes with respect to risk assessment and risk management, and shall assess the steps management has taken to monitor and control such risks, except with respect to those risks for which oversight has been assigned to other committees of the Board or retained by the Board. The Committee shall review the Company's annual disclosures concerning the role of the Board in the risk oversight of the Company.
>
> [emphasis added]

45. The same duties are also recognized in the Corporate Governance Guidelines of 23andMe, dated May 18, 2023.

46. The Individual Defendants breached their duties, and through action and/or omission, materially contributed to the events leading to the Data Breach and the Data Breach itself.

c) KPMG LLP

i. KPMG's Engagement with 23andMe

47. The Defendant KPMG is a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

48. At the relevant time, KPMG were the independent auditors of 23andMe from KPMG's offices located in Santa Clara, California.

49. At the relevant time, the audit engagement partner of KPMG in relation to 23andMe was Katie Wechsler. Ms. Wechsler has over 20 years of experience working for KPMG in the U.S., the U.K., and Switzerland, serving a wide range of companies, both listed and private. Ms. Wechsler has extensive experience managing the audits of multinational companies within the life sciences, consumer markets, and technology sectors. Her existing client base includes both public and private life sciences companies.

ii. KPMG Promoted 23andMe and Used Its Relationship with 23andMe to Promote Its Own Business Interests

50. KPMG has been a promoter of 23andMe Defendants' business, and actively promoted the significant commercial and corporate value in the interconnected genomic and health data they possessed on customers.

51. The global member firms of KPMG have significant involvement with, and actively promote, the companies that operate in the life sciences sector. The KPMG global members' website maintains a dedicated page for life sciences, available at https://kpmg.com/xx/en/home/industries/life-sciences.html, which extensively promotes KPMG's services in relation to this sector.

52. Amongst other things, this section of KPMG Global website discusses the "Future of life sciences" and argues: "[t]he future of life sciences will likely be shaped by tech-enabled connectivity, strategic uses of AI, and patient-centric supply chains

… leaders are rethinking their operating models to ensure they can meet stakeholder expectations, anticipate threats, and capitalize on data-driven insights to win in the marketplace."

53. This section of KPMG Global website provides a link to a paper titled "**The future of life sciences; Pressing issues and critical imperatives that will shape the new model for the industry—the connected life sciences company**." This paper notes that the development of "precision medicine" with the use of "individuals' unique genetic profiles and, in some cases, engineers a therapy from a patient's own cells" as amongst one of the critical signals of the change in the industry, again promoting the commercial capabilities of the exact same kind of data 23andMe Defendants possessed on customers.

54. This paper is co-authored by Larry Raff, a partner with KPMG US, and the KPMG Global Head of Life Sciences and the KPMG US National Market line of business leader. Mr. Raff has over 20 years delivering large scale business, risk and technology transformations to major companies around the world. His focus is on how innovation and changes in market dynamics can help transform outcomes. He has significant depth and expertise in business transformation, process redesign, reactive and predictive risk analysis and innovation-led transformations

55. In a further paper titled "**Driving value from genomics in Life Sciences**," KPMG International furthermore promotes the significance and usage of the customer data collected and generated by 23andMe Defendants, and argues: "Genomic data [is] the most personal of all human data … the way such information is gathered, stored, analyzed and used [has] led to a change" in the industry.

56. This paper specifically refers to the licensing arrangements between 23andMe and GSK and promotes the corporate and commercial value in this transaction, noting that the use of the 23andMe Defendants' data increased the chance of success in the development of pharmaceuticals.

57. This paper is also co-authored by the KPMG Global Head of Life Sciences and the KPMG US National Market line of business leader, Mr. Raff.

58. A further paper published by KPMG member firms titled "**Reshaping the future of pharma: Four critical capabilities for 2030**" further discusses the opportunities and risks in the use of "data-rich" pharmaceutical developments, and further promotes the significant value of the data collected and generated by 23andMe Defendants.

iii. KPMG Was Aware of The Data Privacy and Cybersecurity Risks Associated with 23andMe's Business

59. KPMG member firms have extensively commented on these topics, including without limitation in a paper titled "**Direct-to-consumer genetic testing; Opportunities and risks in a rapidly evolving market**," which amongst other things represented as follows:

> The global direct-to-consumer genetic testing market is growing, fuelled by a rise in awareness, an emerging culture of consumer empowerment, and the demand for increasingly personalized services. However, companies offering these services face increasing concern over data privacy and scientific validity. We advise existing and potential players to focus on building consumer trust, to tailor services to maximize consumer satisfaction, and to work together with regulatory bodies if they hope to thrive in this market.
>
> Direct-to-consumer genetic testing: an exciting market, but not without its challenges.
>
> Once purely the domain of healthcare institutions, rapid technological advancement over the last decade has made it possible for genetic testing to be undertaken cheaply, quickly and directly by consumers.
>
> The global direct-to-consumer genetic testing (DTC-GT) market is forecast to grow steadily to be worth over US$1bn by 20201 , but commercial success for new and more established players is not guaranteed. A set of wide-ranging challenges are likely to become more acute as regulation tightens. For example, growing concerns over data privacy, scientific accuracy, and the

> psychological impact on consumers demands careful consideration.
>
> Genomic data is special, since it encodes not only our blueprint, but that of our family and children. The continuing privacy and the security of people's genetic data, both immediately, and into the long term, is of paramount importance.

60. The significance of the data privacy and cybersecurity practices was also known to Ms. Wechsler, the KPMG audit partner in charge of the 23andMe engagement. In 2023, at the exact same time that the Data Breach affecting 23andMe was being carried out, Ms. Wechsler made the following post on her public social media:

> Fraud, non-compliance and cyber-attacks: These overlapping risks are a triple threat for all organizations. New research from #KPMG suggests that Life Sciences companies may be at greater risk due to overconfidence and underinvestment. Here are five things Life Sciences executives need to know.
>
> #fraud #forensic #lifesciences #investigations #fincrimes #financialcrimes

61. Ms. Wechsler's post provided a link to a KPMG paper titled "**Life Sciences: KPMG 2022 Fraud Outlook A triple threat across the Americas**," which found, amongst other things, that "Cyber security is another area for this industry where extensive risk and overconfidence co-exist."

E. The Data Breach

62. For the purposes of this Amended Notice of Civil Claim, the term Data Breach refers to the event, or the sequence of events occurring between April 29, 2023 and September 27, 2023, whereby unauthorized parties exploited the vulnerabilities in the design and structure of the 23andMe Defendants' systems and improperly accessed and obtained highly sensitive and highly valuable personal and health information of the 23andMe Defendants' customers. The Data Breach was first widely reported in the media in early October 2023, following which the 23andMe Defendants commenced an investigation into the

Data Breach. On December 5, 2023, the 23andMe Defendants reported that they had completed their investigation into the Data Breach.

63. On or about October 6, 2023, the 23andMe Defendants published a post on their website titled "Addressing Data Security Concerns," stating as follows:

> **Addressing Data Security Concerns**
>
> We recently learned that certain 23andMe customer profile information that they opted into sharing through our DNA Relatives feature, was compiled from individual 23andMe.com accounts without the account users' authorization.
>
> After learning of suspicious activity, we immediately began an investigation. While we are continuing to investigate this matter, we believe threat actors were able to access certain accounts in instances where users recycled login credentials – that is, usernames and passwords that were used on 23andMe.com were the same as those used on other websites that have been previously hacked.
>
> We believe that the threat actor may have then, in violation of our Terms of Service, accessed 23andMe.comaccounts without authorization and obtained information from certain accounts, including information about users' DNA Relatives profiles, to the extent a user opted into that service.
>
> **Committed to Safety and Security**
>
> 23andMe is committed to providing you with a safe and secure place where you can learn about your DNA knowing your privacy is protected. We are continuing to investigate to confirm these preliminary results. We do not have any indication at this time that there has been a data security incident within our systems, or that 23andMe was the source of the account credentials used in these attacks.
>
> At 23andMe, we take security seriously. We exceed industry data protection standards and have achieved three different ISO certifications to demonstrate the strength of our security program. We actively and routinely monitor and audit our systems to ensure that your data is protected. When we receive information through those processes or from other sources claiming customer data has been accessed by unauthorized individuals, we immediately investigate to validate whether this information is accurate. Since 2019 we've offered and

encouraged users to use multi-factor authentication (MFA), which provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords.

Recommendations

We encourage our customers to take as much action to keep their account and password secure. Out of caution, we recommend taking the following steps:

- Confirm you have a strong password, one that is not easy to guess and that is unique to your 23andMe account. If you are not sure whether you have a strong password for your account, reset it by following the steps outlined here.
- Please be sure to enable multi-factor authentication (MFA) on your 23andMe account. You can enable MFA by following the steps outlined here.
- Review our Privacy and Security Checkup page with additional information on how to keep your account secure.

23andMe is here to support you. Please contact Customer Care at customercare@23andme.com if you need assistance with navigating these important steps to protect your account.

64. The 23andMe Defendants' October 6, 2023 statements were updated on or about October 9, 2023 to include the following statements:

Update: October 9, 2023 8:25 PM PST

What actions has 23andMe taken?

Our investigation continues and we have engaged the assistance of third-party forensic experts. We are also working with federal law enforcement officials.

We are reaching out to our customers to provide an update on the investigation and to encourage them to take additional actions to keep their account and password secure. Out of caution, we are requiring that all customers reset their passwords and are encouraging the use of multi-factor authentication (MFA).

If we learn that a customer's data has been accessed without their authorization, we will notify them directly with more information.

Please continue to follow this blog for updates as our investigation continues.

F. Customer Data Becomes Available for Sale on Dark Web

65. The Dark Web is a corner of the internet that is generally not public-facing or available to ordinary audience. The Dark Web participants cannot be readily tracked, and can thus take advantage of anonymity and anonymous activity. Given these features, the Dark Web is actively used by cybercriminals to carry out criminal activities, amongst other purposes.

66. Threat actors began advertising 23andMe customer data for sale on a Dark Web marketplace forum known as the BreachForums on or about October 2, 2023.

67. A web posting on the Dark Web, which is attributed to the threat actors, dated October 16, 2023, states and alleges that the threat actor had been able to access and obtain troves of highly sensitive personal and health information of, allegedly, all of the 23andMe Defendants' customers.

68. On or about October 6, 2023, the media reported that customer information of approximately 1 million Ashkenazi Jewish and 100,000 Chinese customers of 23andMe had been made available for sale on the Dark Web. The 23andMe Defendants confirmed those reports.

69. The media reported that the cause(s) of the breach and the full scope of the breach was(ere) still unknown.

70. Of note, these reports surfaced at the same time as the conflict in the Middle East was triggered by an attack against Israel, raising significant concerns and distress amongst the Jewish community.

71. According to the alleged hacker, the data stolen and made available for sale on the Ashkenazi Jewish customers of the 23andMe Defendants included such information as profile id, account id, first name, last name, sex, birth year, detailed geographic location information as well as genomic data. The hacker further

alleged that they possessed information on all of 23andMe Defendants' customers.

72. On or about October 18, 2023, the threat actors made available for sale the highly sensitive personal information of approximately 4.1 million further customers of 23andMe. They, furthermore, claimed that the data set included DNA profiles of the customers, including that of notable public figures and dignitaries.

73. The threat actors claimed the data set included information such as name, date of birth, gender, email and genetic ancestry.

74. It is reported that the threat actor was selling the data for £8 per item, if bought in the blocks of 100,000, or up to $100 per profile, and that the data included associated email addresses.

75. In the aftermath of these reports, investigative media reported that they had been able to confirm that the 23andMe Defendants' customer data had been made available for sale on the Dark Web as early as on August 11, 2023. According to these reports, a hacker claimed to have 300 terabytes of stolen 23andMe data for sale. The hacker further alleged that they had contacted the 23andMe Defendants, but that the Defendants had not taken the matter seriously. It is reported that the batch of the customer data presented in this incident included genetic data of certain senior Silicon Valley executives.

76. In December 2023, the 23andMe Defendants admitted that the Data Breach had resulted in the compromise of the highly sensitive and valuable personal and health information of at least 6.9 million of their customers. According to the 23andMe Defendants, the threat actor was able to access the accounts of approximately 14,000 of their customers through credential stuffing attacks, and then used those account "to access the information included in a significant number of DNA Relatives profiles (approximately 5.5 million) and Family Tree feature profiles (approximately 1.4 million), each of which were connected to the compromised accounts."

77. On or about January 25, 2024, the 23andMe Defendants admitted in a regulatory filing with the Attorney General of California that the Data Breach has occurred, and it went unnoticed, from April 29, 2023 through to September 27, 2023.

78. In breach notifications sent to customers in or around January 2024, the 23andMe Defendants also acknowledges that the threat actors were able to access raw genotype or genetics data and health reports.

G. Data Breach Methodology

79. The 23andMe Defendants state that their investigation into the Data Breach is ongoing.

80. The 23andMe Defendants initially claimed that the Data Breach was carried out through the "credential stuffing" method. In the credential stuffing method, the threat actor would collect generally available information from the victims and cross-reference them to other breached databases or aggregated data, and recycle re-used passwords in order to be able to compromise their accounts.

81. The 23andMe Defendants contend that customer data had been scraped from publicly available sections of their website, and improperly misused through the "credential stuffing" method of attack.

82. Despite the 23andMe Defendants' contention, it is doubted that credential stuffing would have been the root cause, or alternatively the sole contributing cause, of the Data Breach. In light of the breadth and scope of the breach, and the fact that the threat actors have accessed and stolen the information of at a minimum one third of the 23andMe Defendants' customers, there is reason to believe that the Data Breach was carried out through penetrating the 23andMe Defendants' systems and/or otherwise accessing database servers or backup drives, amongst other possible methods.

83. But even if the Data Breach was carried out through credential stuffing, the 23andMe Defendants' improper and inadequate measures of control were a

contributing factor. Specifically, the 23andMe Defendants failed to impose multi-factor authentication, nor did they implement safeguard measures on their website to prevent data scraping, nor did they shield their systems against automated and repeated access attempts or requests, all contrary to the standards applicable to the retention and protection of the highly sensitive and highly valuable personal information in their control, possession or custody.

H. The Standards Applicable to the 23andMe Defendants in Managing and Safeguarding Customers' Highly Sensitive Personal Information, Which They Violated

84. To provide their offerings and services, the 23andMe Defendants require and collect highly sensitive personal and health information from customers including, without limitation, significant information concerning their ethnical backgrounds, ancestral roots and connections, religion, and human genome.

85. There can be no doubt that the information that the 23andMe Defendants collect from their customers, or generate on customers in the course of providing its offerings and services, are highly sensitive and confidential. Indeed, the Defendants (including the Individual Defendants and KPMG) have consistently acknowledged the sensitivity of the customer information that it 23andMe collects from, or generates on, its customers in the course of its business activities.

86. The 23andMe Defendants are subject to specific laws, regulations and industry standards and practices to properly manage customer data and to safeguard it against unauthorized access or theft, as detailed below. In broad terms, the applicable standards required the 23andMe Defendants to:

a. disclose the specific purposes for which they collected customer data and obtain the customer's informed, express consent for such use;

b. retain and use the information only for the specified purposes and as long as the information is necessary or required to fulfill such specified purposes;

c. dispose of the information once it was no longer required for the specified purposes; and

d. while the information remained in the 23andMe Defendants' control, custody or possession, to use appropriate and adequate safeguard measures to protect the information against unauthorized access or theft.

a) The 23andMe Defendants Acknowledge They Are Subject to Rigorous Privacy and Data Security Regulation

87. The 23andMe Defendants' filings with the United States Securities and Exchange Commission acknowledge in great detail that they are subject to rigorous data privacy and data protection regulations, including notably Canada's federal private sector privacy legislation, *PIPEDA*.

88. The 23andMe Defendants' Annual Report on Form 10-K for the fiscal year ending March 31, 2023, states as follows:

> *Privacy and Security Regulation*
>
> We are engaged in ongoing privacy compliance and oversight efforts, including in connection with the requirements of numerous local, state, federal and international laws, rules, and regulations relating to the privacy and security of directly or indirectly identifiable personal information (collectively, "Data Protection Laws"). Such Data Protection Laws regulate the collection, storage, sharing, use, disclosure, processing, transferring, and protection of personal information, including genetic information, and evolve frequently in scope and enforcement. There can also be uncertainty, differing interpretations, and potentially contradictory requirements across the privacy and security legal and regulatory landscape. In the U.S., some of the notable Data Protection Laws we are subject to include the California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively, the "CCPA"), the California Genetic Information Privacy Act ("GIPA"), California Confidentiality of Medical Information Act ("CMIA"), Section 5 of the Federal Trade Commission Act ("FTC Act"), the Telephone Consumer Protection Act of 1991 ("TCPA") and, in the event of a data breach, various data breach laws across the 50 states and territories. Outside of the U.S., numerous countries have their

own Data Protection Laws, including, but not limited to, the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA") and the EU General Data Protection Regulation ("GDPR"), now also enacted in the U.K. ("UK GDPR"). 23andMe also expects additional Data Protection Laws to be proposed and enacted in the future, particularly in the U.S., and current Data Protection Laws to evolve frequently through new legislation and amendments to existing legislation and changes in enforcement approach. The effects of such changes may be inconsistent from one jurisdiction to another, and potentially far-reaching and may require us to modify our data processing practices and policies and incur substantial compliance-related costs and expenses. These new or modified Data Protection Laws, and other changes in laws or regulations relating to privacy, data protection and information security, particularly any new or modified laws or regulations that require enhanced protection of certain types of data or new obligations or restrictions with regard to data retention, transfer or disclosure and the use of data for research purposes, could greatly increase the cost of providing our offerings, require significant changes to our operations or even prevent us from providing certain offerings in jurisdictions in which we currently operate and in which we may operate in the future. Additionally, many of the Data Protection Laws give rights to control how data is used to the user and this is a potential significant business cost for us.

Data Protection Laws are enforced by the FTC, government authorities and agencies, including state attorneys general and national or state data protection authorities. Data Protection Laws require us to publish statements or notices to our customers that describe how we handle personal information and provide details of the choices that customers have about the way we handle their personal information and of their rights. If such information that we publish is considered untrue or inaccurate, we may be subject to claims of unfair or deceptive trade practices under Section 5 of the FTC Act or similar laws, which could lead to significant liabilities and consequences.

[…]

Internationally, we are subject to, among other Data Protection Laws, the GDPR, UK GDPR, and PIPEDA which regulate collection, storage, sharing, use, disclosure, and protection of personal information, and impose stringent requirements with significant penalties and litigation risks for noncompliance. Like the U.S., international Data Protection Laws include national, state or provincial, and local laws, meaning compliance costs

increase with every state, province, or locale we ship to. Failure to comply with the GDPR (and the UK GDPR) may result in fines of up to €20 million/£17.5 million or up to 4% of the annual global revenue of the infringer, whichever is greater. It may also lead to civil litigation, with the risks of damages or injunctive relief, or regulatory orders adversely impacting the ways in which our business can use personal information. While Canada's PIPEDA does not have as stringent requirements and fines as the GDPR at this time, Canadian legislators are actively working on reforms to PIPEDA to align it with the GDPR. We anticipate that any reforms to PIPEDA will further increase our compliance costs and liabilities.

b) The Standards Applicable to the 23andMe Defendants Under Canadian Law Applicable to Collection and Use of Genetic Information, Which They Violated

89. On May 4, 2017, Bill S-201, the *Genetic Non-Discrimination Act*, SC 2017, c 3 ("***Genetic Non-Discrimination Act***") received Royal Assent.

90. The *Genetic Non-Discrimination Act* prohibits any person from requiring an individual to undergo a genetic test or to disclose the existing results of genetic tests. This law empowers customers to retain and exercise control over their personal information, and prohibits all persons from collecting, using or disclosing the genetic test results without the customer's written consent.

91. Furthermore, the *Genetic Non-Discrimination Act* prohibits any person from requiring an individual to undergo a genetic test or disclose the results of a genetic test as a condition of providing goods or services to, entering into or continuing a contract or agreement with, or offering specific conditions in a contract or agreement with, the individual.

92. The 23andMe Defendants violated the foregoing standards as a result of the following actions and omissions:

a. misrepresenting their data retention practices, or otherwise failing to implement proper data retention practices. Specifically, the Defendants retained large troves of highly sensitive and highly valuable customer data

that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and

b. misrepresenting their data protection practices, or otherwise failing to implement proper data protection practices. Specifically, the Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks

93. Each of the Individual Defendants and KPMG acted together with the 23andMe Defendants in actions, omissions and breaches of the duties that violated the standards applicable under the *Genetic Non-Discrimination Act*.

94. As a result of the Defendants' actions and omissions in breach of their duties, the Defendants enabled, caused or prompted the Data Breach, affirmatively exposing and granting access to the putative Class Members' highly sensitive and highly valuable personal information to unauthorized third parties and cybercriminals.

95. The Defendants' actions and omissions contrary to the standards applicable under the *Genetic Non-Discrimination Act* constituted deliberate and purposeful conduct, which was carried out in the context of a for-profit commercial and/or customer relationship with putative Class Members, and in furtherance of or consistent with the Defendants' commercial goals and interests.

c) The Standards Applicable to the 23andMe Defendants Pursuant to *PIPEDA*, Which They Violated

96. As entities that are engaged in the collection, use and disclosure of personal information in the course of commercial activities in Canada, the 23andMe Defendants are subject to the *PIPEDA*.

97. The *PIPEDA* applies to entities that are in control of personal information. In this case, the 23andMe Defendants were in control of the Class Members' personal information.

98. Schedule 1 of the *PIPEDA* required that that the 23andMe Defendants conduct themselves in accordance with the following statutory duties:

a. section 4.1 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must be responsible and accountable for personal information, and that they must implement policies and practices to give effect to the principles concerning the protection of personal information;

b. section 4.2 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must identify the purposes for which personal information was collected at the time or before personal information was collected;

c. section 4.3 of Schedule 1 of the *PIPEDA* required that knowledge and consent of the individual Class Members were required for the collection, use or disclosure of personal information, and that the 23andMe Defendants were required to make a reasonable effort to ensure that the individual Class Members were advised of the purposes for which personal information was collected;

d. section 4.3.2 of Schedule 1 of the *PIPEDA* required that the individual Class Members' consent be "meaningful," further requiring that "the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed";

e. sections 4.3.5 and 4.3.8 of Schedule 1 of the *PIPEDA* specified that the Class Members' reasonable expectations were relevant to obtaining consent, and that they ought to have been afforded the opportunity, subject to legal or contractual restrictions and reasonable notice, to withdraw consent;

f. section 4.5 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants were not permitted to use or disclose the personal information for any purposes other than those for which it was collected, except with the Class Members' consent;

g. section 4.5.3 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must destroy, erase or anonymize the personal information that was no longer required to fulfill the identified purpose, and that the 23andMe Defendants must develop guidelines and implement procedures to govern the destruction of personal information; and

h. section 4.7 of Schedule 1 of the *PIPEDA* required that the 23andMe Defendants must protect the personal information by security safeguards appropriate to its sensitivity against loss or theft, as well as unauthorized access, disclosure, use, or modification.

99. The 23andMe Defendants violated the foregoing standards as a result of the following actions and omissions:

a. misrepresenting their data retention practices, or otherwise failing to implement proper data retention practices. Specifically, the 23andMe Defendants retained large troves of highly sensitive and highly valuable customer data that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and

b. misrepresenting their data protection practices, or otherwise failing to implement proper data protection practices. Specifically, the 23andMe Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.

100. Each of the Individual Defendants and KPMG acted together with the 23andMe Defendants in actions, omissions and breaches of the duties that violated the standards applicable under the *PIPEDA*.

101. As a result of the Defendants' actions and omissions in breach of their duties, the Defendants enabled, caused or prompted the Data Breach, affirmatively exposing and granting access to the putative Class Members' highly sensitive and highly valuable personal information to unauthorized third parties and cybercriminals.

102. The Defendants' actions and omissions contrary to the standards applicable to them under *PIPEDA* constituted deliberate and purposeful conduct, which was carried out in the context of a for-profit commercial and/or customer relationship with putative Class Members, and in furtherance of or consistent with the Defendants' commercial goals and interests.

d) The Industry Standards Applicable to the 23andMe Defendants, Which They Violated

103. The 23andMe Defendants are based in, and operate from, the United States, and are subject to the standards promulgated or recommended by the United States Federal Trade Commission ("**FTC**").

104. FTC has published guidelines and recommendations to business regarding the appropriate practices to safeguard customer information. FTC recommends that the need for data security should be factored into all business decision-making.

105. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

106. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

107. The 23andMe Defendants violated the foregoing standards as a result of the following actions and omissions:

    a. misrepresenting their data retention practices, or otherwise failing to implement proper data retention practices. Specifically, the 23andMe Defendants retained large troves of highly sensitive and highly valuable customer data that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and

    b. misrepresenting their data protection practices, or otherwise failing to implement proper data protection practices. Specifically, the 23andMe Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.

108. Each of the Individual Defendants and KPMG acted together with the 23andMe Defendants in actions, omissions and breaches of the duties that violated the above-noted industry standards.

109. As a result of the Defendants' actions and omissions in breach of their duties, the Defendants enabled, caused or prompted the Data Breach, affirmatively exposing and granting access to the putative Class Members' highly sensitive and highly valuable personal information to unauthorized third parties and cybercriminals.

110. The Defendants' actions and omissions contrary to the industry standards constituted deliberate and purposeful conduct, which was carried out in the

context of a for-profit commercial and/or customer relationship with putative Class Members, and in furtherance of or consistent with the Defendants' commercial goals and interests.

e) The Standards Applicable to the 23andMe Defendants Pursuant to Their Own Policies, Statements and Representations, Which They Violated

111. The 23andMe Defendants recognize the highly sensitive nature of the information they collect from or on their customers.

112. The 23andMe Defendants' customer-facing website includes a section titled "Data Protection," which states that "23andMe is committed to the robust data privacy and security protections enabled by GDPR compliance." Even though this section of the 23andMe Defendants' website specifically addresses the European GDPR, the website and the Defendants' representations made therein are accessible in Canada, and the same representations are made to the 23andMe Defendants' Canadian customers. In any event, the standards applicable to safeguarding customer information is substantively similar across the various jurisdictions in which the 23andMe Defendants operate.

113. At all material times, the 23andMe Defendants also maintained a stated Privacy Statement, which promised and represented that "At 23andMe, Privacy is in our DNA."

114. The 23andMe Defendants' Privacy Statement, furthermore, contained statements and representations substantially as follows:

> **How we use your information**
>
> Now that we've covered the types of information we collect and how we collect it, let's review how we may use it. As a reminder, we will not use your Genetic Information for personalized or targeted marketing and/or advertising without your explicit consent. If you want to dig into the details of how we use your information, check out our How We Use Your Information page.
>
> **We use your information to:**

- Provide our Services, including to develop, operate, improve, maintain, and safeguard our Services, including developing new product tools and features
- Analyze and measure trends and usage of the Services
- Communicate with you, including customer support, or to share information about our Services or other offers or information we think may be relevant to you
- Personalize, contextualize and market our Services to you
- Provide cross-context behavioral or targeted advertising (learn more in our Cookie Policy and Cookie Choices page)
- Enhance the safety, integrity, and security of our Services, including prevention of fraud and other unauthorized or illegal activities on our Services
- Enforce, investigate, and report conduct violating our Terms of Service or other policies
- Conduct surveys or polls, and obtain testimonials or stories about you
- Comply with our legal, licensing, and regulatory obligations
- Conduct 23andMe Research, if you choose to participate

[…]

How does 23andMe protect my information in Research?

23andMe Research analyses are conducted with information that has been stripped of your identifying Registration Information. You can read more about protections for your data in the Main Research Consent.

[…]

Who we *DO NOT* share with:

You can rest assured, *we will not* voluntarily share your Personal Information with:

- Public databases
- Insurance companies or employers
- Law enforcement, absent a valid court order, subpoena, or search warrant (Check out our track record on this promise in our Transparency Report)

[…]

Security Measures

We implement physical, technical, and administrative measures aimed at preventing unauthorized access to or disclosure of your Personal Information. Our team regularly reviews and improves our security practices to help ensure the integrity of our systems and your Personal Information. To learn more about our practices, please visit our Customer Care guidance.

Please recognize that protecting your Personal Information is also your responsibility. Be mindful of keeping your password and other authentication information safe from third parties, and immediately notify 23andMe of any unauthorized use of your login credentials. Your password is not visible to 23andMe staff, and we encourage you not to share your password with 23andMe or any third parties. 23andMe cannot secure Personal Information that you release on your own or that you request us to release.

[…]

Retention of Personal Information

We retain Personal Information for as long as necessary to provide the Services and fulfill the transactions you have requested, comply with our legal obligations, resolve disputes, enforce our agreements, and other legitimate and lawful business purposes. Because these needs can vary for different data types in the context of different services, actual retention periods can vary significantly based on criteria such as user expectations or consent, the sensitivity of the data, the availability of automated controls that enable users to delete data, and our legal or contractual obligations.

23andMe and/or our contracted genotyping laboratory will retain your Genetic Information, date of birth, and sex as required for compliance with applicable legal obligations, including the federal Clinical Laboratory Improvement Amendments of 1988 (CLIA), California Business and Professions Code Section 1265 and College of American Pathologists (CAP) accreditation requirements, even if you chose to delete your account. 23andMe will also retain limited information related to your account and data deletion request, including but not limited to, your email address, account deletion request identifier, communications related to inquiries or complaints and legal agreements for a limited period of time as required by law, contractual obligations, and/or as necessary for the establishment, exercise or defense of legal claims and for audit and compliance purposes.

115. The 23andMe Defendants violated the foregoing promises, statements, representations and standards as a result of the following actions and omissions:

    a. misrepresenting their data retention practices, or otherwise failing to implement proper data retention practices. Specifically, the Defendants retained large troves of customer data that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and

    b. misrepresenting their data protection practices, or otherwise failing to implement proper data protection practices. Specifically, the Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.

116. Each of the Individual Defendants and KPMG acted together with the 23andMe Defendants in actions, omissions and breaches of the duties that violated the standards outlined in 23andMe's own Privacy Statement.

117. As a result of the Defendants' actions and omissions in breach of their duties, the Defendants enabled, caused or prompted the Data Breach, affirmatively exposing and granting access to the putative Class Members' highly sensitive and highly valuable personal information to unauthorized third parties and cybercriminals.

118. The Defendants' actions and omissions contrary to their promises, statements and representations constituted deliberate and purposeful conduct, which was carried out in the context of a for-profit commercial and/or customer relationship with putative Class Members, and in furtherance of or consistent with the Defendants' commercial goals and interests.

f) The Defendants Violated the Applicable Standards Knowingly, Wilfully or Recklessly

119. The 23andMe Defendants are a publicly traded company involved in the highly sensitive biotechnology sector. They The 23andMe Defendants describe themselves as the pioneers in providing in direct-to-consumer genetic testing, and they possess one of the most significant databases of human genome in the world.

120. The Individual Defendants are highly skilled and sophisticated persons with unparalleled experience in the tech and life sciences industry sectors.

121. KPMG is a member of the one of the largest global audit and consultancy firms (one of the "Big 4"), with unparalleled resources and expertise, including in relation to audit, internal controls and governance relevant to computer systems and data management.

122. The Defendants are highly sophisticated corporate and individual actors, who are aware of both the value of the information they the 23andMe Defendants collect as well as the value of that information to outside parties, including criminals.

123. The Defendants knew at all times, or they ought to have known, that the trove of highly valuable and sensitive personal information they the 23andMe Defendants collect, generate and store on customers is an extremely attractive target to cybercriminals.

124. The Defendants knew at all times, or they ought to have known, that they the 23andMe Defendants were exposed to a heightened risk of cyberattacks.

125. The Defendants knew at all time, or they ought to have known, that unauthorized access to, or theft of, the highly sensitive customer information in they the 23andMe Defendants' possession, power or control would expose the customers to a real and immediate risk of significant privacy harms, damages and losses, including:

a. identity theft;

b. financial harms, including damages to credit ratings or creditworthiness;

c. reputational harms;

d. relationship harms; and/or

e. physical harms.

126. The Defendants acknowledged that they the 23andMe Defendants had an obligation to implement, maintain and utilize appropriate technical, technological and procedural safeguard in order to protect the highly sensitive customer information in their power, possession or custody.

127. The data and information security vulnerabilities that enabled the Data Breach were in the design and structure of the 23andMe Defendants' systems. The 23andMe Defendants had made deliberate choices in the design and structure of their systems and website.

128. Furthermore, the 23andMe Defendants were advised of the vulnerabilities in the design and structure of their computer systems, but they chose to disregard those vulnerability reports. The 23andMe Defendants' decision to disregard those reports was deliberate and purposeful.

129. The Data Breach was as such the fruit of the 23andMe Defendants' deliberate and purposeful choices and decisions as to how to design and build their systems, and how to respond (or not to respond) to the reports of vulnerabilities in 23andMe Defendants' computer systems.

130. The Defendants took upon themselves the risk that unauthorized parties or criminals would access or otherwise compromise the highly sensitive and highly valuable customer information in the 23andMe Defendants' power, possession or custody.

131. The Defendants failed to act to protect the putative Class Members' highly sensitive and highly valuable personal information appropriate to the sensitivity of that information and the risks of cyberattacks. The Defendants' actions and omissions were carried out with the knowledge of the real and far-reaching adverse consequences of their breaches of duties.

132. In failing to design and build the systems reasonably free from vulnerabilities, and in failing to reasonably respond to the reports of such vulnerabilities, the Defendants failed to conduct themselves appropriate to the sensitivity of the customer information in their power, possession or custody and the severity of the risk of cyberattacks. The Defendants' conduct was wilfull, knowing or, alternatively, and/or reckless. The Defendants' conduct was thus willful.

g) The 23andMe Defendants' Detection and Response to the Data Breach Improper and Inadequate

133. As part of their overall data accountability, retention and protection practices, the 23andMe Defendants were subject to standards requiring them to detect and respond to any incident of compromise of customer data without delay and in a proper way. The 23andMe Defendant failed to comply with those standards.

134. It is currently unknown when the Data Breach occurred. In January 2024, the 23andMe Defendants reported that the Data Breach occurred from April 2023 through to September 2023.

135. It is unknown whether the 23andMe Defendants became aware of the Data Breach by themselves or after the media or other third parties reported that their customer data was available for sale on the Dark Web.

136. However, the 23andMe Defendants failed to detect the Data Breach by themselves. There are reports of at least two distinct threat actors who reported that they had identified and exploited the vulnerability in the 23andMe Defendants' systems design and structure between August and October 2023. Both of them reported that they had reported the vulnerabilities to the 23andMe

Defendants, but that the 23andMe Defendants failed to take those issues seriously. The sequence of events suggests that the 23andMe Defendants began investigating the Data Breach later during the first week of October 2023, when the media widely reported that threat actors had accessed and were selling 23andMe customer data on the Dark Web.

137. Given the highly sensitive nature of the customer data, no delay in the detection, response to, or communication regarding the Data Breach would be warranted.

138. Still, it took the 23andMe Defendants several days to acknowledge the Data Breach, and still several more days to communicate regarding the Data Breach with their customers.

139. Yet still, the 23andMe Defendants' communication has been inadequate and inappropriate, as they have failed to provide accurate or complete information to customers regarding what information has been exposed and how customer have been affected.

140. Nor have the 23andMe Defendants provided accurate or complete information regarding the events leading to the Data Breach and the subsequent events.

141. None of that is justified in the circumstances, given the customer data is literally available on the Dark Web.

142. The 23andMe Defendants' improper and inadequate response to the Data Breach indicates that they did not have a proper data security incident response plan.

143. In regulatory filings with the Attorney General of California, filed in January 2024, the 23andMe Defendants acknowledged that the Data Breach had occurred over the span of approximately five months, and that it went undetected, from April through to September 2023.

144. To date, the 23andMe Defendants have not advised customers how and in what ways they have been affected in the Data Breach. Additionally, the 23andMe

Defendants have not advised their customers whose information was posted on the Dark Web that they have been affected in such way.

145. The 23andMe Defendants' communication to their customer regarding the Data Breach has been improper and/or inadequate.

I. 23andMe Defendants Collected, Used and Retained Customer Data Beyond Authorization

146. The 23andMe Defendants collected, retained and used customer data beyond authorization, and without the customers' informed explicit consent in accordance with the standards applicable under the *Genetic Non-Discrimination Act* and the *PIPEDA*.

147. A material purpose and a fundamental value proposition underpinning 23andMe Defendants' business was to monetize on customers' highly valuable genetic and health data. The 23andMe Defendants actively sought to drive commercial value and profit from customer data in their possession.

148. The use of customer data for these purposes was specifically raised with, and commented on by, Ms. Wojcicki in an interview titled "23andMe Admits 'Mining' Your DNA Data Is Its Last Hope," dated February 13, 2024. In this interview, Ms. Wojcicki was quoted as saying "We now have the ability to mine the dataset for ourselves, as well as to partner with other groups. It's a real resource that we could apply to a number of different organizations for their own drug discovery."

149. When asked whether, in her view, "customers are aware that opting in to research also means opting in to giving pharmaceutical partners their data," Ms. Wojcicki refused to provide a direct answer but instead stated as follows: "It's not individual-level data, unless they explicitly consented for individual-level data. I think that most people want to see improvements in their lives," attempting to ascribe an "implied consent" to 23andMe customers.

150. 23andMe Defendants did not, and do not, have the requisite informed, explicit consent of its customers to mine their data for highly profitable pharmaceutical activities. Thus, they collected, accumulated, stored and used customer data beyond and in excess of authorization and of purposes other than those contemplated by customers.

J. The Defendants' Misrepresentations

a) The 23andMe and Individual Defendants

151. The 23andMe Defendants and Individual Defendants made both misrepresentations alleged herein:

a. that the 23andMe Defendants employed proper and effective data retention measures and practices; and

b. that the 23andMe Defendants employed proper and effective data protection measures and practices.

152. Those misrepresentations were made, whether explicitly or implicitly, and whether by omission or commission, in: (a) 23andMe's Privacy Statement; (b) 23andMe's filings with regulators; and (c) in public statements made by the Individual Defendants, which they made on their own behalf and under the authority and on behalf of 23andMe.

153. Those misrepresentations were material to the promotion of 23andMe Defendants' offerings and services. But for the promise of privacy the customers would not provide 23andMe Defendants with their DNA samples and highly sensitive personal and health information.

b) KPMG

154. KPMG made both misrepresentations alleged herein:

c. that the 23andMe Defendants employed proper and effective data retention measures and practices; and

d. that the 23andMe Defendants employed proper and effective data protection measures and practices.

155. KPMG made the foregoing misrepresentations to the public, whether explicitly or implicitly, and whether by omission or commission, in its papers, including those identified herein: (a) “Driving value from genomics in Life Sciences”; and (b) “Reshaping the future of pharma Four critical capabilities for 2030.”

156. KPMG furthermore made the foregoing misrepresentations in the presentations, results of factual inquiries and investigations and opinions provided to 23andMe Defendants and their directors and officers, including the Individual Defendants. And those representations were incorporated in 23andMe Defendants and Individual Defendants’ statements and regulatory filings.

157. KPMG furthermore made the foregoing misrepresentations to the public, whether explicitly or implicitly, and whether by omission or commission, in KPMG’s audit reports, KPMG’s audit report on 23andMe dated May 25, 2023 recognized and represented as follows:

> A company’s internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. **A company’s internal control over financial reporting includes those policies and procedures that** (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) **provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the**

> **company's assets that could have a material effect on the financial statements.**
>
> …
>
> ***in our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of March 31, 2023 …***
>
> [bold added and italics]

158. Those misrepresentations were material to the promotion of 23andMe Defendants' offerings and services. But for the promise of privacy the customers would not provide 23andMe Defendants with their DNA samples and highly sensitive personal and health information.

K. The Plaintiff and Putative Class Members Have Suffered Harms, Damages and Losses

159. The Class Members' information has been stolen by criminals. At a minimum, the information of a subset of the Class Members, namely the members of the Sub-Class, has been made available for sale on the Dark Web.

160. The Plaintiffs and putative Class Members have suffered, and will continue to suffer, harms, damages and losses as a result of the Defendants' misrepresentations and its conduct, as particularized herein.

161. In order to provide their its services and offerings, the 23andMe Defendants require and collect highly sensitive personal information on their customers. Additionally, in the course of the customer relationship, and in the normal course of carrying out their business, the 23andMe Defendants generate highly sensitive personal information on their customers.

162. The highly sensitive information the 23andMe Defendants collect from and/or generate on their customers is highly valuable generally and specifically in the context of the within case. Dark Web pricing indices indicate that the personally

identifiable information that was affected in the within case can have a Dark Web market price of up to thousands of dollars.

163. The Plaintiffs and putative Class Members entrusted the 23andMe Defendants with their highly sensitive, valuable personal information. But for the Defendants' promises, representations and statements, the Plaintiffs and putative Class Members would not have purchased the 23andMe Defendants' offerings or services.

164. The Data Breach was preventable. But for the Defendants' acts, omissions and breaches of the duty in violation of their promises, representations and statements, and but for the Defendants' violation of the standards applicable to them in safeguarding the Class Members' highly sensitive personal information, the Data Breach would not have occurred.

165. The Plaintiffs and the putative Class Members have suffered the following harms, damages and losses:

a. economic loss and deprivation equal to the monetary consideration paid for the 23andMe Defendants' offerings and services;

b. economic loss and deprivation equal to the "premium" paid for the 23andMe Defendants' offerings and services in order to safeguard customer information;

c. loss of valuable, confidential personal and commercial information, all of which is intrinsically valuable;

d. damages stemming from, or caused by, identity fraud schemes including, without limitation, damage to credit ratings, damage to perceive credit worthiness, reputation, relationship and other personal and commercial interests;

e. non-pecuniary harms, damages and losses as a result of the Data Breach, including emotional distress and anxiety;

f. out of pocket expenses required to respond to the consequences of the Data Breach;

g. loss of valuable time and resources required to respond to the consequences of the Data Breach; and/or

h. being exposed to a real risk of significant harm as a result of the exposure of highly sensitive personal and commercial information.

L. Any Restrictive Term or Clause Invalid as Unconscionable or Due to Public Policy Considerations, or Otherwise Unenforceable

166. Any restriction on the Plaintiffs and/or putative Class Members in bringing this class action by way of the 23andMe Defendants' terms of service, including any class action waiver clause, is invalid or otherwise unenforceable due to the Defendants' misrepresentations, as alleged herein.

167. Furthermore, or in the alternative, any such restriction is invalid or otherwise unenforceable due to the 23andMe Defendants' material breach of the contract in all material respects.

168. Furthermore, or in the alternative, any such restriction is invalid or otherwise unenforceable due to the significant imbalance of bargaining power between the putative Class Members and the 23andMe Defendants. The 23andMe Defendants unilaterally impose the terms of the contract with the Class Members. Those terms are not open to negotiation. The 23andMe Defendants may, and they do, unilaterally change the terms of service. The 23andMe Defendants' contract with the putative Class Members is a standard form contract, to which the doctrine of *contra proferentem* applies.

169. Furthermore, or in the alternative, any such restriction is invalid or otherwise unenforceable because the within claim concerns privacy and quasi-constitutional rights and interests. The 23andMe Defendants may not contract

out of the putative Class Members' right to enforce their quasi-constitutional rights and interests in Canadian Courts.

170. Furthermore, or in the alternative, any such restriction is invalid or otherwise unenforceable because the within claim concerns consumer or consumer-like interests. The 23andMe Defendants did not bring such restrictions to the attention of the putative Class Members or, alternatively, failed to properly and adequately explain to them the effect of such restrictive clauses.

171. Furthermore, or in the alternative, any such restriction is invalid or otherwise unenforceable by reason of public policy because class action waiver and similar restrictive clauses are contrary to good governance, effectively extinguish or substantively restrict access to justice, are contrary to behaviour modification and are also contrary to judicial economy.

M. Canadian Regulators' Investigation

172. On June 10, 2024, the Office of the Privacy Commissioner of Canada announced a joint investigation, together with the privacy regulators of the United Kingdom, into 23andMe's Data Breach. Of note, this announcement seemed to indicate that concurrent investigations were also being undertaken by provincial privacy regulators of British Columbia, Alberta and Québec.

173. In relation to this announcement, the Office of the Privacy Commissioner of Canada underscored the highly sensitive nature of the information in the possession of 23andMe, and the material harms and significant risks of harms that may result of the improper exposure of that information.

PART 2 3: RELIEF SOUGHT

1. On behalf of himself themselves and the Class, the Plaintiffs seeks:

    a. an order anonymizing the Plaintiffs's identity through initializing their his names;

b. an order pursuant to all applicable provisions of the *Class Proceedings Act*, RSBC 1996, c. 50, including, but not limited to, sections 2, 4, 4.1, 5, 6, 7, 8, and 10 thereof, certifying this action as a multi-jurisdictional class proceeding and appointing the Plaintiff as the Representative Plaintiff for the Class, defined as follows:

> All natural persons residing or domiciled in Canada whose sensitive personal information was accessed by unauthorized parties or otherwise compromised in the course of or as a result of the Data Breach;
>
> The Class includes a Sub-Class defined as follows: all natural persons residing or domiciled in Canada whose sensitive personal information was accessed by unauthorized parties or otherwise compromised in the course or as a result of the Data Breach, whose information was posted on the Dark Web;
>
> Excluded from the Class are the directors, partners, officers or senior employees of the 23andMe Defendants, KPMG or any of their respective subsidiaries;
>
> or such other class definition as may be proposed by the Plaintiff or approved by the Court;

c. monetary compensation to the Class for general, compensatory, consequential, symbolic, moral, aggravated, punitive or other forms of damages, whether statutory, at common law and/or equity, on an aggregated basis to the fullest extent possible, for:

   i. **as against each of the Defendants,** breaches of **Provincial Privacy Legislation**:

1. on behalf of individual Class Members residing in British Columbia, pursuant to section 1 of the *Privacy Act*, RSBC 1996, c. 373, as amended;

2. on behalf of individual Class Members residing in Manitoba, pursuant to section 2 of *The Privacy Act*, CCSM c P125, as amended;

3. on behalf of individual Class Members residing in Newfoundland and Labrador, pursuant to section 3 of the *Privacy Act*, RSNL 1990, c P-22, as amended;

4. on behalf of individual Class Members residing in Quebec, pursuant to articles 3 and 35-37 of the *Civil Code of Québec*, CQLR c CCQ-1991, section 5 of the *Charter of Human Rights and Freedoms*, CQLR c C-12, section 10 of the *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1, each as amended; and

5. on behalf of individual Class Members residing in Saskatchewan, pursuant to section 2 of *The Privacy Act*, RSS 1978, c P-24, as amended;

ii. **as against each of the Defendants,** the tort of intrusion upon seclusion, on behalf of individual Class Members residing in Canadian Provinces and Territories other than British Columbia, Manitoba, Newfoundland and Labrador, Quebec, and Saskatchewan;

iii. **as against each of 23andMe Holding Co. and 23andMe, Inc.,** breaches of **Provincial Consumer Legislation**, as identified below, giving rise to remedy or relief for monetary compensation, recission, disgorgement of profits or similar relief under the statutes identified below, or otherwise providing the basis for relief at law and/or equity,

including without limitation, under the doctrine of waiver of tort, based on the Defendant's breaches of the statutory rights, mandates, duties, obligations or prohibitions identified below:

1. on behalf of Class Members residing in British Columbia: Part 2 of the *Business Practices and Consumer Protection Act*, SBC 2004, c 2, as amended, and sections 1, 2, 4, 5, 7, 8, 9, 10, 12, 14, 171, and/or 172 thereof;

2. on behalf of Class Members who reside in Alberta, the *Consumer Protection Act*, RSA 2000, c F-2, as amended, and sections 1, 2, 5, 6, 7, 7.2, 13, 20, 21, 22, 23, and/or 142.1 thereof;

3. on behalf of Class Members who reside in Manitoba, *The Business Practices Act*, CCSM, c B120, as amended, and sections 1, 2, 3.1, 4, 5, 6, 7, 8, and/or 23 thereof;

4. on behalf of Class Members who reside in Newfoundland and Labrador, the *Consumer Protection and Business Practices Act*, SNL 2009, c C-31.1, as amended, and sections 2, 7, 8, 9, and/or 10 thereof;

5. on behalf of Class Members who reside in Nova Scotia, the *Consumer Protection Act*, RSNS 1989, c 92, as amended, and sections 26, 27, and/or 28 thereof;

6. on behalf of Class Members residing in Ontario: *Consumer Protection Act*, 2002, SO 2002, c 30, Sch A, as amended, and sections 1, 14, 15, 17, 18, 116, and/or 117 thereof;

7. on behalf of Class Members who reside in Prince Edward Island, the *Business Practices Ac*t, RSPEI 1988, c B-7, as amended, and sections 1, 2, 3, and/or 4 thereof;

8. on behalf of Class Members who reside in Quebec, the *Consumer Protection Act*, CQLR, c P-40.1, as amended, and sections 1, 2, 11.1, 37, 40, 41, 42, 53, 54, 215, 216, 217, 218, 219, 220, 221, 223.1, 228, 238, 239, 252, 253, 262, 263, 271, 272, and/or 276 thereof; and

9. on behalf of Class Members who reside in Saskatchewan, *The Consumer Protection and Business Practices Act*, SS 2013, c C-30.2, as amended, and sections 2, 4, 5, 6, 7, 8, 9, 15, 44, 45, 91, and/or 93 thereof;

granting statutory injunctions, restraining orders and/or restoration orders, furthermore waiving notice requirements, if any, where appropriate under applicable Provincial Consumer Legislation; and

iv. **as against each of 23andMe Holding Co. and 23andMe, Inc.,** breach of contract, on behalf of all Class Members;

v. **as against each of the Defendants,** negligence, on behalf of all Class Members;

vi. **as against each of the Defendants,** pursuant to section 36(1) of the *Competition Act*, RSC 1985, c C-34, breaches of Part VI, section 52, of the *Competition Act*, RSC 1985, c C-34, on behalf of all Class Members; and

vii. **as against each of the Defendants,** vicarious, agency, common enterprise and/or joint-tortfeasor liability;

d. an order directing a reference or giving such other directions as may be necessary to determine issues not determined at the trial of the common issues;

e. pre-judgment and post-judgment interest pursuant to the *Court Order Interest Act*, RSBC 1996, c.79;

f. costs of this action; and

g. such further and other relief as this Honourable Court may deem just.

PART 3 4 : LEGAL BASIS

A. Material Facts Pleaded Herein and Incorporated by Reference

1. The Plaintiffs incorporates, repeats and pleads herein the pleadings contained in Parts 1, 2 and 3 hereof.

2. Specifically, and without limiting the generality of the foregoing, the Plaintiffs pleads and asserts that the 23andMe Defendants are subject to rigorous data privacy and security obligations. The applicable standards were informed by:

   a. The *Genetic Non-Discrimination Act*, SC 2017, c 3;

   b. The *PIPEDA*;

   c. Industry practices, including the standards promulgated by the FTC; and

   d. The 23andMe Defendants' own statements and policies, including their stated Privacy Statement.

3. Furthermore, and without limiting the generality of the foregoing, the Plaintiffs pleads and asserts that the 23andMe Defendants violated the standards applicable to them as a result of the following actions and omissions:

   a. misrepresenting their data retention practices, or otherwise failing to implement proper data retention practices. Specifically, the 23andMe Defendants retained large troves of highly sensitive and highly valuable customer data that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and

b. misrepresenting their data protection practices, or otherwise failing to implement proper data protection practices. Specifically, the 23andMe Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.

4. The Individual Defendants made material misrepresentations to the public in relation to 23andMe's data retention measures and practices, as well as its data protection measures and practices. They did so in order to promote the use of 23andMe's services and product offerings.

5. KPMG made material misrepresentations to the public in relation to 23andMe's data retention measures and practices, as well as its data protection measures and practices. It did so in order to promote the use of 23andMe's services and product offerings. It further did so in order to promote its own services and offerings, including with those relevant to the design and/or assessment and audit of data privacy and cybersecurity measures.

6. Each of the Defendants materially contributed to the events leading to and resulting in the Data Breach. But for the actions, omissions and breaches of duties of each of the Defendants, the Data Breach would not have occurred. The Defendants acted jointly as co-principals and/or co-conspirators, and in an integrated scheme, and materially contributed to the design of, and/or assessment and audit of, as well as making representations to the public regarding the propriety and efficacy of, 23andMe's data privacy and cybersecurity measures.

7. The Defendants' actions and omissions in breach of their duties constituted deliberate and purposeful conduct on the part of the Defendants, which was carried out in furtherance, as part of and/or in the normal course of carrying out their business.

8. The Defendants were aware of the heightened risk of cybersecurity and the significant harm to customers from the compromise of the sensitive data in 23andMe Defendants' possession. The Defendants took upon themselves the risk that customer data may be compromised and accessed by unauthorized parties, including cybercriminals. They failed to act or take action to protect the putative Class Members' highly sensitive and highly valuable personal information appropriate to the sensitivity of that information or the severity of the risk of cyberattacks.

9. The Defendants' conduct was willful, as it was knowing and/or, alternatively, reckless, in that:

   a. the Data Breach was the result of specific, known or identifiable security vulnerabilities within 23andMe's computer systems' design and structure;

   b. the 23andMe Defendants' choices relevant to the design and structure of their computer systems were deliberate and purposeful, and they were made consistent with and in furtherance of their business;

   c. the 23andMe Defendants furthermore chose to not address or rectify those vulnerabilities. Their failure to rectify the security vulnerabilities, in the face of actual or constructive knowledge of them, and in the face of the known and understood material risks arising from data security incidents, constituted deliberate and purposeful conduct; and

   d. the Individual Defendants and KPMG acted as co-principals and joint tortfeasors in the violation of the duties pertaining to the design and/or assessment of 23andMe's computer systems in the course of their ordinary commercial, for-profit activities, deliberately and purposefully.

10. As a result of the Defendants' actions and omissions in breach of their promises, statements, representations and duties, the Defendants enabled, caused or prompted the Data Breach, affirmatively exposing and granting access to the

putative Class Members' highly sensitive and highly valuable personal information to unauthorized third parties and cybercriminals.

11. The putative Class Members' highly sensitive and highly valuable personal information has been made available for sale on the Dark Web.

12. The Plaintiffs and the putative Class Members have incurred actual harms, damages and losses, including emotional harms, as a result of the Defendants' conduct, and are exposed to further risks of significant harm.

B. Breaches of Provincial Privacy Legislation

13. On behalf of himself and all other Class Members who are individuals residing in British Columbia, Manitoba, Newfoundland and Labrador, Quebec, and Saskatchewan, the Plaintiff J. R. pleads the statutory rights of action available under the Provincial Privacy Legislation.

14. This cause of action is being pleaded and asserted against each of the Defendants.

15. For the purposes of these claims brought pursuant to the Provincial Privacy Legislation, the Plaintiff J. R. pleads and identifies the applicable provisions of the statutes which are identified in Part 3, para 1(c)(i) of this Notice of Civil Claim.

16. The Defendants violated the Plaintiff J. R.'s and putative Class Members' privacy.

17. The Defendants violated the Plaintiff J. R.'s and putative Class Members' privacy willfully. Specifically, the Defendants' actions and omissions were not appropriate to the sensitivity of the information or the severity of risks of cyberattacks. As such, the Defendants' conduct was deliberate and purposeful, and it was knowing or, alternatively, reckless.

18. The Defendants violated the Plaintiff J. R.'s and putative Class Members' privacy without a claim of right. Specifically, as the Plaintiff and Class Members had a reasonable expectation—as confirmed in the Defendants' own statements and

representations—that the Defendants would properly manage, retain and protect the data. The Defendants had no justification in retaining data beyond the scope of their authorization, and/or in failing to implement proper technical, technological and/or procedural measures and controls to safeguard the putative Class Members' highly sensitive and highly valuable personal information.

C. Tort of intrusion upon seclusion

19. On behalf of herself and all Class Members who are individuals residing in Canadian jurisdictions that do not have provincial privacy legislation, the Plaintiff M. M. pleads and asserts the tort of intrusion upon seclusion.

20. This cause of action is being pleaded and asserted against each of the Defendants.

21. In support of this claim, the Plaintiff M. M. pleads and asserts that the Defendants intruded upon these Class Members' privacy in a way that was offensive to a reasonable person and caused distress, humiliation, or anguish by:

    a. misrepresenting their 23andMe's data retention measures and practices, or otherwise failing to implement proper data retention practices. Specifically, the 23andMe Defendants retained large troves of highly sensitive and highly valuable customer data that they no longer required to maintain for a valid purpose, and/or otherwise outside of the scope of their authorization; and

    b. misrepresenting their 23andMe's data protection measures and practices, or otherwise failing to implement proper data protection practices. Specifically, the 23andMe Defendants failed to introduce, implement and/or maintain appropriate technical, technological and/or procedural measures and controls to safeguard customer data appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.

22. The 23andMe Defendants accumulated, stored, retained, used, and/or disclosed the Plaintiff's and putative Class Members' highly sensitive and highly valuable

personal information for reasons other than those reasonably contemplated by putative Class Members.

D. Breaches of Provincial Consumer Legislation

23. On behalf of himself themselves and all putative Class Members residing in British Columbia, Alberta, Manitoba, Newfoundland and Labrador, Nova Scotia, Ontario, Prince Edward Island, Quebec and Saskatchewan, the Plaintiffs pleads and asserts a claim for damages pursuant to Provincial Consumer Legislation.

24. This cause of action is being pleaded and asserted against 23andMe Holding Co. and 23andMe, Inc.

25. For the purposes of these claims brought pursuant to the Provincial Consumer Legislation, the Plaintiffs pleads and identifyies the applicable provisions of the statutes which are identified in Part 3, para 1(c)(iii) of this Notice of Civil Claim.

26. Each Class Member is a “consumer” within the meaning of the Provincial Consumer Legislation and for the purposes of this claim.

27. Each Class Member’s transaction whereby they paid to use the 23andMe Defendants’ offerings or services is a “consumer transaction” within the meaning of the Provincial Consumer Legislation and for the purposes of this claim.

28. Each 23andMe Defendant is a “supplier” within the meaning of the Provincial Consumer Legislation and for the purposes of this claim.

29. The 23andMe Defendants engaged in deceptive and unfair acts and practices, and made misrepresentations for the purposes of promoting their offerings and services by way of:

    a. misrepresenting 23andMe’s their data retention measures and practices; and

    b. misrepresenting 23andMe’s their data protection measures and practices.

30. These Defendants were enriched through the consumer transactions as a result of the payments they received for their offerings and services.

31. As a result of the breaches of the Provincial Consumer Legislation, the consumer transactions are not binding on these Class Members.

32. Each Class Member has an interest in the funds paid by them and received by the 23andMe Defendants for use of their offerings and services, has an interest in the restoration of those amounts, and has a right to make a claim for damages.

33. Each Class member is entitled to a declaration that the 23andMe Defendants engaged in deceptive conduct and, where applicable, an injunction, restraining order and/or restoration order.

E. Breach of contract

34. On behalf of themselves himself and all putative Class Members, the Plaintiffs pleads and asserts breach of contract.

35. This cause of action is being pleaded and asserted against 23andMe Holding Co. and 23andMe Inc.

36. The Plaintiffs and Class Members entered into an actual and/or implied contract with the 23andMe Defendants, which contained the following material terms, whether explicitly or implicitly:

    a. that the 23andMe Defendants would introduce, implement and maintain proper data retention measures and practices, and to not retain customer data beyond authorization; and

    b. that the 23andMe Defendants would introduce, implement and maintain proper data protection measures and practices through proper technical, technological and procedural measures and controls appropriate to the sensitivity of the information and the severity of the risk of cyberattacks.

37. These Defendants violated those material terms of the contract.

38. The Plaintiffs and putative Class Members suffered harms, damages, and losses as a result of the 23andMe Defendants' breach of contract.

39. The Plaintiffs's and putative Class Members' contract with the 23andMe Defendants is a contract of adhesion to which the doctrine of *contra proferentem* applies.

F. Negligence

40. On behalf of themselves himself and all putative Class Members, the Plaintiffs pleads and asserts a claim in common law negligence.

41. This cause of action is being pleaded and asserted against each of the Defendants.

42. The Plaintiffs and the putative Class Members were in a special relationship with each of the Defendants as customers of the 23andMe Defendants.

43. The Plaintiffs and the putative Class Members were known or knowable, and identified or identifiable to each of the Defendants.

44. The Defendants owed a duty of care to the Plaintiffs and the putative Class Members to implement proper data retention and data protection measures and practices.

45. The Defendants jointly and materially contributed to the defective state of 23andMe's data privacy and cybersecurity measures and practices either by virtue of designing and/or overseeing the design of, and/or assessing and/or overseeing the assessment or audit of those measures and practices.

46. The Defendants jointly and materially contributed to the misrepresentations made to the wide array of public audience, including the regulators, customers and

23andMe's other stakeholders regarding the propriety and efficacy of 23andMe's data privacy and cybersecurity measures.

47. The Defendants acted as co-principals and/or co-conspirators, in tandem and in an integrated scheme to design, assess, and make material misrepresentations to the public that 23andMe's data privacy and cybersecurity measures were proper and effective, while they were not.

48. It was reasonably foreseeable to the Defendants that the Plaintiffs and putative Class Members would suffer harms, damages, and losses if the Defendants breached their promises, statements, representations or otherwise duty of care, which they did.

49. The Defendants were on notice of a heightened risk of cyberattacks against them, and that the Plaintiffs and putative Class Members would suffer severe consequences, harms, losses, and damages if the Defendants breached their duty of care, which they did.

50. The Defendants chose to conduct themselves in a manner that was not appropriate to the sensitivity of customer data and/or the severity of the risk of cyberattacks. The Defendants' conduct was deliberate and purposeful, in furtherance or in the course of conducting their business, and. it It was thus knowing or, alternatively, willful or reckless and, thus, willful.

51. The Plaintiffs and the putative Class Members had no control over the Defendants' decisions and conduct, but trusted that the Defendants would introduce, implement and maintain proper data retention and protection measures. Indeed, the Defendants promised, stated and represented that they would do so.

52. The Plaintiffs and the putative Class Members suffered harms, damages, and losses as a result of the Defendants' breaches of their duty of care.

G. Breach of Part VI of the *Competition Act*

53. On behalf of themselves himself and all other Class Members, the Plaintiffs pleads and asserts a claim for damages pursuant to section 36 of the *Competition Act* against the Defendants arising out of their violation of Part VI, section 52 of the *Competition Act*.

54. This cause of action is being pleaded and asserted against each of the Defendants.

55. The Defendants made representations to the public that were false or misleading in a material respect regarding the propriety and efficacy of their data retention and data protection practices.

56. The Defendants made those false or misleading representations for the purpose of promoting, directly or indirectly, the supply or use of their offerings and services, and/or or for the purpose of promoting, directly or indirectly, their business interests, knowingly or recklessly.

57. If and to the extent the Plaintiffs and/or putative Class Members need to prove reliance and/or causation, reliance and causation:

    a. may be inferred, given the nature and ordinary use of the information with which the Plaintiffs and the putative Class Members entrusted the Defendants;

    b. may be established directly and by inference based on the Defendants' own statements and representations acknowledging the significance of their privacy and data security obligations commensurate to the putative Class Members' privacy interests, and that they are accordingly subject to rigorous data privacy and data security regulation; and/or

    c. may be established directly by the Plaintiffs and each putative Class Member through individual assessments, which can be done through an efficient and manageable process to be established.

H. Vicarious, Agency, Common Enterprise and Joint-Tortfeasor Liability

58. In addition to their direct liability, each Defendant is vicariously liable for the actions and omissions of its co-defendant and that of its operating companies, subsidiaries, partners, and their respective directors, officers, employees, and agents.

59. The Data Breach did not happen accidentally, but it happened due to the Defendants' organizational failures to employ proper data retention and data protection measures and practices. The Defendants acted in tandem, as co-principals, co-conspirators and joint tortfeasors in the violation of the applicable duties. They each made a material contribution to the Data Breach. But for the actions, omissions and breaches of duties on the part of each of the Defendants, the Data Breach would not have occurred.

60. If and to the extent the Defendants' impugned actions and omissions are attributable to their directors, officers or employees, the Defendants are vicariously liable, because they created the risk of failure in safeguarding the customer data in their power, custody or possession.

61. The risk was foreseeable, indeed known and acknowledged by the Defendants. The risk was created due to the Defendants' conduct and its actions and omissions. The Defendants foresaw, allowed and/or tolerated the occurrence of the risk within their organization in the course of their ordinary business activities and in furtherance of their business and commercial interests.

62. The risk materialized when the Data Breach occurred, exposing the highly sensitive and highly valuable personal information of the Class Members to unauthorized parties and cybercriminals.

I. The Plaintiffs and Class Members Are Entitled to Compensation

63. As pleaded herein in Part 2, paragraphs 90-96, the Plaintiffs and putative Class Members have incurred harms, damages and/or losses as a result of the Defendants' conduct.

64. The Plaintiffs and putative Class Members plead that they are entitled to monetary awards or compensation under common law, statutory and/or equitable headings of damages.

65. In the alternative, the Plaintiffs and putative Class Members plead entitlement to compensation under waiver of tort or for disgorgement of profits, and claim an accounting or such other restitutionary relief as may be available for all revenues or profits generated by the Defendants from, as a result of, or reasonably connected with its violations contractually and at law to protect their private information.

66. The Plaintiffs's and Class's compensation may be assessed and determined by the Court through expert evidence, including evidence of economists, assessor and/or insurance actuaries.

Plaintiffs's address for courier service:

Sage Nematollahi (he/him)
c/o YLAW GROUP
410-1122 Mainland Street
Vancouver, BC V6B 5L1

Place of trial: Vancouver, British Columbia.

The address of the registry is: 800 Smithe Street, Vancouver, BC V6Z 2E1.

Date: September 18, 2024

KND Complex Litigation.

KND COMPLEX LITIGATION
Yonge Eglinton Centre
Suite 401, 2300 Yonge Street
Toronto, Ontario M4P 1E4
T: (416) 537-3529

Eli Karp (he/him)
ek@knd.law

Sage Nematollahi (he/him)
sn@knd.law

YLAW GROUP
410-1122 Mainland Street
Vancouver, BC V6B 5L1
T: (604) 974-9529

Leena Yousefi (she/her)
leena@ylaw.ca

Counsel to the Plaintiffs

Rule 7-1(1) of *the Supreme Court Civil Rules* states:

> (1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,
>
> > (a) prepare a list of documents in Form 22 that lists
> >
> > > (i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and
> >
> > > (ii) all other documents to which the party intends to refer at trial, and
> >
> > (b) serve the list on all parties of record.

ENDORSEMENT ON ORIGINATING PLEADING OR PETITION
FOR SERVICE OUTSIDE BRITISH COLUMBIA

There is a real and substantial connection between British Columbia and the facts alleged in this proceeding. The Plaintiff and the Class Members plead and rely upon the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28 (the "*CJPTA*") in respect of the Defendants. Without limiting the foregoing, a real and substantial connection between British Columbia and the facts alleged in this proceeding exists pursuant to section 10 of the *CJPTA* because this proceeding:

(e) concerns contractual obligations, and

(i) the contractual obligations, to a substantial extent, were to be performed in British Columbia;

(f) concerns restitutionary obligations that, to a substantial extent, arose in British Columbia;

(g) concerns a tort committed in British Columbia; and

(h) concerns a business carried on in British Columbia.

APPENDIX

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a proposed customer privacy class action arising out of a data breach that affected millions of customers of the Defendants 23andMe in 2023. As a result of the Data Breach, cybercriminals accessed highly sensitive and highly valuable personal information of the Defendants' 23andMe's customers, including information concerning their ethnicities, religious backgrounds, ancestry roots and connections, and genetics. The Plaintiffs alleges that the Defendants did not have proper data retention, data protection measures and practices, and that they failed to conduct themselves appropriate to the sensitivity of the customer information in their power, custody or possession, or the severity of the risk of cyberattacks. The Plaintiffs further allege that the Individual Defendants and KPMG acted as co-principals and/or co-conspirators in an integrated scheme, and materially contributed to the design of, and/or assessment and audit of, as well as making representations to the public regarding the propriety and efficacy of, 23andMe's data privacy and cybersecurity measures. The Plaintiffs and the putative Class seek compensation under common law, statutory, and/or equitable headings of damages.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

[ ] a motor vehicle accident
[ ] medical malpractice
[ ] another cause

A dispute concerning:

[ ] contaminated sites
[ ] construction defects
[ ] real property (real estate)
[ ] the provision of goods or services or other general commercial matters
[ ] investment losses

[ ] an employment relationship

[ ] a will or other issues concerning the probate of an estate

[X] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[X] a class action
[ ] maritime law
[ ] aboriginal law
[ ] constitutional law
[ ] conflict of laws
[ ] none of the above
[ ] do not know

Part 4: ENACTMENTS RELIED ON:

1. *Class Proceedings Act*, RSBC 1996, c. 50, as amended
2. *Court Jurisdiction and Proceedings Transfer Act*, RSBC 2003, c.28, as amended
3. *Genetic Non-Discrimination Act*, SC 2017, c 3;
4. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, as amended
5. *Privacy Act*, RSBC 1996, c. 373, as amended
6. *The Privacy Act*, CCSM c P125, as amended
7. *Privacy Act*, RSNL 1990, c P-22, as amended
8. *Civil Code of Québec*, CQLR c CCQ-1991, as amended
9. *Charter of Human Rights and Freedoms*, CQLR c C-12, as amended
10. *Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1, as amended
11. *The Privacy Act*, RSS 1978, c P-24, as amended
12. *Competition Act*, RSC 1985, c C-34, as amended
13. *Business Practices and Consumer Protection Act*, SBC 2004, c 2, as amended
14. *Consumer Protection Act*, RSA 2000, c F-2, as amended
15. *The Business Practices Act*, CCSM, c B120, as amended

16. *Consumer Protection and Business Practices Act*, SNL 2009, c C-31.1, as amended

17. Nova Scotia, the *Consumer Protection Act*, RSNS 1989, c 92, as amended

18. *Consumer Protection Act*, 2002, SO 2002, c 30, Sch A, as amended

19. *Business Practices Ac*t, RSPEI 1988, c B-7, as amended

20. *Consumer Protection Act*, CQLR, c P-40.1, as amended

21. *The Consumer Protection and Business Practices Act*, SS 2013, c C-30.2, as amended

22. *Court Order Interest Act*, RSBC 1996, c.79, as amended